SUPREME COURT OF THE STATE OF WASHINGTON

DOUG AND BETH O'NEILL, individuals

Respondents,

v.

THE CITY OF SHORELINE, a Washington municipal corporation, and DEPUTY MAYOR MAGGIE FIMIA, individually and in her official capacity,

Petitioners.

AMICUS CURIAE BRIEF OF THE STATE OF WASHINGTON

ROBERT M. MCKENNA Attorney General

Alan D. Copsey, WSBA No. 23305 Deputy Solicitor General PO Box 40100 Olympia, WA 98504-0100 360-664-9018 alanc@atg.wa.gov

TABLE OF CONTENTS

I.	IDENTITY AND INTEREST OF AMICUS CURIAE			
II.	ISSUES			
III.	ARGUMENT			
	A.	The Public Records Act Does Not Require Production Of A Requested Record In Any Specific Format	2	
	B.	A Request To Inspect Or Copy An E-mail Should Not Be Construed As A Request To Inspect Or Copy "Metadata" Associated With The E-mail	4	
	C.	A Request For "Metadata" Ordinarily Is Not A Request For An Identifiable "Public Record" Under The Public Records Act	8	
		"Metadata" Has No Fixed Meaning And Does Not Refer To Any Specific Information	8	
		2. Most "Metadata" Is Not Related To The Conduct Of Government	11	
		3. The Court Should Refrain From Importing Electronic Discovery Rules Into The Public Disclosure Context	14	
IV.	CC	DNCLUSION	19	

TABLE OF AUTHORITIES

Cases

Amren v. City of Kalama, 131 Wn.2d 25, 929 P.2d 389 (1997)17
Beal v. City of Seattle, 150 Wn. App. 865, 209 P.3d 872 (2009)11
Bonamy v. City of Seattle, 92 Wn. App. 403, 960 P.2d 447 (1998), review denied, 137 Wn.2d 1012 (1999)
Dilley v. Metro. Life Ins. Co., 256 F.R.D. 643 (N.D. Cal. 2009)
Hangartner v. City of Seattle, 151 Wn.2d 439, 90 P.3d 26 (2004)
Hearst Corp. v. Hoppe, 90 Wn.2d 123, 580 P.2d 246 (1978)
Kay Beer Distrib., Inc. v. Energy Brands, Inc., No. 07-C-1068, 2009 WL 1649592 (E.D. Wis. June 10, 2009)
Kentucky Speedway, LLC v. NASCAR, Inc., 2006 WL 5097354 (E.D. Ky. 2006)
Koenig v. City of Des Moines, 158 Wn.2d 173, 142 P.3d 162 (2006)1
Limstrom v. Ladenburg, 136 Wn.2d 595, 963 P.2d 869 (1998)
Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534 (D. Md. 2007)
Mancia v. Mayflower Textile Servs. Co., 253 F.R.D. 354 (D. Md. 2008)

Mechling v. City of Monroe, 152 Wn. App. 830 (2009)
Michigan First Credit Union v. Cumis Ins. Soc'y, Inc., 2007 WL 4098213 (E.D. Mich. 2007)17
Oxford House, Inc. v. City of Topeka, 2007 WL 1246200 (D. Kan. 2007)15
York v. Wahkiakum Sch. Dist. 200, 163 Wn.2d 297, 178 P.3d 995 (2008)14
Yousoufian v. Office of Ron Sims, 152 Wn.2d 421, 98 P.3d 463 (2004)17
Zubulake v. UBS Warburg, 217 F.R.D. 309 (S.D.N.Y. 2003)
<u>Statutes</u>
Laws of 1973, ch. 1, § 211
Laws of 1992, ch. 139, § 1
Laws of 1992, ch. 139, § 124
RCW 40.14.0609
RCW 40.14.0709
RCW 42.17.020(42)11
RCW 42.56 1
RCW 42.56.010(2)11
RCW 42.56.070(1)
RCW 42.56.080

RCW 42.56.100						
RCW 42.56.550(4)						
RCW 42.56.570(2)						
Other Authorities						
Bryan A. Garner, Black's Law Dictionary 598 (9th ed. 2009)5						
Computer History Museum, Timeline of Computer History (http://www.computerhistory.org/timeline/?category=sl)11						
Conor R. Crowley and Sherry B. Harris, eds., <i>The Sedona Conference</i> Glossary: E-Discovery & Digital Information Management, Second Edition 19 (2nd ed., Dec. 2007)						
Craig Ball, Meeting the Challenge: E-Mail in Civil Discovery (2008)						
Diane Hillman, Dublin Core® Metadata Initiative, <i>Using</i> Dublin Core (2007)						
Ian Peter, The History of E-mail (http://www.nethistory.info/ History%20of%20the%20Internet/email.html)						
Jonathon M. Redgrave et al., eds., The Sedona Principles: Best Practices, Recommendations & Principles for Addressing Electronic Document Production (2nd ed. 2007)						
Kevin F. Brady et al., eds., The Sedona Conference [®] Commentary on ESI Evidence & Admissibility, 8 Sedona Conf. J. 239 (Mar. 2008)						
Lucia Cucu, The Requirement for Metadata Production Under Williams v. Sprint/United Management Co.: An Unnecessary Burden for Litigants Engaged in Electronic Discovery, 93 Cornell L. Rev. 221 (2007)						

•		
	Mia Mazza et al., In Pursuit of FRCP 1: Creative Approaches to Cutting and Shifting the Costs of Discovery of Electronically Stored Information, 13 Rich. J.L. & Tech. 11 (2007)	
	Richard T. Griffiths, History of Electronic Mail (http://www.let.leidenuniv.nl/history/ivh/chap3.htm)11	
	Rodney A. Satterwhite & Matthew J. Quantrara, Asymmetrical Warfare: The Cost of Electronic Discovery in Employment Litigation, 14 Rich. J.L. & Tech. 9 (2008)	
	Thomas Y. Allman, The Impact of the Proposed Federal E-Discovery Rules, 12 Rich. J.L. & Tech. 1 (2006)	
	Washington State Archives, Office of the Secretary of State, "Frequently Asked Questions for Digital WAC 434-662" (2008) 9	
	Rules	
	Fed. R. Civ. P. 26(b)	
t	Fed. R. Civ. P. 26(b)(2)(B)	
	Fed. R. Civ. P. 26(b)(2)(C)	
	Fed. R. Civ. P. 34(b)	•
	Regulations	
	WAC 434-662-0209	
	WAC 44-142	

I. IDENTITY AND INTEREST OF AMICUS CURIAE

Amicus curiae is the state of Washington.

The Public Records Act, RCW 42.56, provides for access to public records to ensure open, transparent, and responsive government. The people of the state and the agencies serving them share this vital interest in government accountability under the Act and in the sound development of case law concerning the Act. The State respectfully submits this amicus brief to assist the Court in reaching a decision in this case that is respectful of the terms of the Act and the Legislature's role in setting policies and provisions to govern public disclosure.

II. ISSUES

This case involves escalating public record requests for a single e-mail. A simple dispute in the trial court has led to issues with potentially broad implications statewide. This brief addresses three such issues:

- 1. Does the Public Records Act require an agency to provide a requested record in a format prescribed by the requester?
- 2. Is a request for an e-mail necessarily also a request for electronic "metadata" associated with that e-mail?
- 3. Is a request for "metadata," without more, a request for an identifiable public record?

III. ARGUMENT

A. The Public Records Act Does Not Require Production Of A Requested Record In Any Specific Format

The Public Records Act does not expressly or impliedly require an agency to provide a requested record in any specific format. *Mechling v. City of Monroe*, 152 Wn. App. 830, 849-50, ¶¶ 35-38 (2009). Rather, the Act confers discretion on an agency to determine how to provide requested records consistent with the agency's duties to (1) delete information that is statutorily exempt from disclosure before producing the records, (2) protect public records from damage or disorganization, and (3) prevent excessive interference with other essential functions of the agency. RCW 42.56.070(1), .100. In the proper exercise of that discretion, an agency may produce a copy in the same format as the original record or it reasonably may determine that an alternative format is more convenient or useful to the requester; more efficient and less expensive; or necessary to facilitate redactions, preparation of a disclosure log, and organized production of records. ¹

¹ The Mechling Court held explicitly that the City "has no express obligation to provide the requested e-mail records in an electronic format". 152 Wn. App. at 850, ¶ 37. Citing a provision in the advisory model rules on public records compliance (WAC 44-14), the Court remanded for a determination whether it was reasonable and feasible for the City to provide requested e-mails in an electronic format. Because the model rules are advisory only, RCW 42.56.570(2), they do not supersede or restrict the discretion conferred by the Act.

The Public Records Act always has been far less concerned with the medium of storage than with the information that has been stored. It always has been permissible under the Act, for example, to provide paper copies of information stored on microfiche. A copy of an old sound recording can be provided in a modern digital format. Handwriting on a page can be photocopied. Old digital files created with programs and systems that now are obsolete can be disclosed through conversion for use by currently-available programs and systems.

In 1992, the Legislature responded incrementally to the increased use and reliance on electronically-stored information by amending the Act's definition of "writing" to include "existing data compilations from which information may be obtained or translated." Laws of 1992, ch. 139, § 1. The 1992 legislation did not set any new standard or adopt any new mandate to treat electronic records differently from paper records, even though the Legislature formally acknowledged that electronic records "pose a number of challenging public disclosure questions," including

how to provide public access to electronic records while balancing personal privacy and vital governmental interests; how to best address requests for electronic records which require agencies to manipulate data; how to open electronic records to public inspection; how to calculate charges for data or products from electronic records, particularly if that data or product is to be used for a commercial purpose; and how public agencies and employees should handle the personal privacy issues associated with electronic mail.

Laws of 1992, ch. 139, § 12. Instead of addressing these questions, the Legislature referred them to a "joint select committee on open government" with directions to report back by January 1, 1993. No report was issued, and the Legislature has not amended the Act to mandate any specific mode of production or special treatment of electronic records.

Even though most information now is generated and stored electronically, the Act continues to treat electronic records as one among many possible means by which information relating to the conduct of government may be created, used, and retained. The Act does not single out special requirements for the production of electronic records; it simply requires that they be disclosed, just as records retained in other forms must be disclosed, leaving state and local agencies with reasonable discretion to determine the appropriate format for production in each instance.

B. A Request To Inspect Or Copy An E-mail Should Not Be Construed As A Request To Inspect Or Copy "Metadata" Associated With The E-mail

An "e-mail" is commonly understood to be the message that appears on a computer screen when one person sends a message to another

person using a computer network.² The message typically includes "header" information ("From," "To," "Cc," "Subject," "Date," etc.), the text of the message, and any pictures, charts, or documents that were inserted in or attached to the e-mail. The author of an e-mail enters the information to be included in the e-mail, then sends it. The person receiving the e-mail may save or delete the message, open and view it, forward or respond to it, or ignore it. To the great majority of people who use computers, the message on the computer screen is the e-mail, and a request for a copy of an e-mail would be satisfied by producing the message that is visible on the computer screen.

On its way from sender to recipient, however, an e-mail message is manipulated by the e-mail program used by the sender, by the e-mail system or systems over which the e-mail is transmitted, and by the e-mail program used by each recipient. Those manipulations recreate the message in electronic code and create additional encoded electronic information about the message that allows the message to be transmitted, received, and displayed on a computer screen.³ These different types of

² In this context, dictionaries that define "e-mail" usually define it as a communication exchanged between *people* over a computer network. *See*, *e.g.*, Bryan A. Garner, *Black's Law Dictionary* 598 (9th ed. 2009).

³ See generally Craig Ball, Meeting the Challenge: E-Mail in Civil Discovery at 11-17 (2008) (at http://www.craigball.com/em2008.pdf). See also Conor R. Crowley and Sherry B. Harris, eds., The Sedona Conference Glossary: E-Discovery & Digital Information Management, Second Edition 19 (2nd ed., Dec. 2007) (noting that the

encoded electronic information may be referred to as examples of "metadata" (although, as explained in the next section of this brief, the term "metadata" is remarkably imprecise and cannot be understood to refer to any specific information).

The electronic coding that allows an e-mail to be transmitted from one computer to another is analogous in some ways to an envelope that allows a letter to be mailed from one address to another. If someone asked for a copy of a letter received by an agency, the appropriate response under the Public Records Act would be to make a photocopy of the letter and give it to the requester (assuming no additional processing is required to redact any information in the letter that is statutorily exempt from disclosure). Having done so in a timely manner, the agency is in full compliance with the Act.

However, the envelope that transmitted the letter might contain more information about the letter—information that might be characterized as "envelope metadata." The envelope might contain additional address information, a postmark indicating date of mailing, and

specific "e-mail metadata" created varies markedly among different systems) (at http://www.thesedonaconference.org/dltForm?did=TSCGlossary_12_07.pdf); Jonathon M. Redgrave et al., eds., The Sedona Principles: Best Practices, Recommendations & Principles for Addressing Electronic Document Production at 3 (2nd ed. 2007) (noting that e-mail "metadata" may contain 1200 or more sets of encoded information) (at http://www.thesedonaconference.org/dltForm?did=TSC_PRINCP_2nd_ed_607.pdf). All Internet sites cited herein were last visited Feb. 12, 2010.

perhaps an electronic bar code added by the Postal Service that could reveal which sorting facility processed the envelope. Nevertheless, a request for the letter would not reasonably be understood as a request for the envelope.

If the envelope had been separately retained as a public record and was specifically identified and requested, then of course it would be subject to disclosure under the Public Records Act. Analogously, where the encoded electronic "header" information has been retained and is specifically identified and requested, it may be subject to disclosure under the Act. But just as a simple record request for a letter is not a request for an envelope, a simple request for an e-mail should not be understood as a request for the encoded electronic information that has been created by the e-mail system or systems sending, transmitting, and receiving the e-mail. Most of this encoded information is not even viewable in the e-mail program (e.g., Microsoft Outlook or an analogue) used to create or view the message, and it is no more a part of the ordinary experience of a person using e-mail than are the electrons moving through a wire to create an electrical current. For normal intents and purposes, it is separate from the message. In the public records context, an e-mail is the message, not the electronic coding used by e-mail systems to transmit the message.

- C. A Request For "Metadata" Ordinarily Is Not A Request For An Identifiable "Public Record" Under The Public Records Act
 - 1. "Metadata" Has No Fixed Meaning And Does Not Refer
 To Any Specific Information

The term "metadata" was registered in 1986 as a trademark belonging to the Metadata Company (U.S. Trademark Registration No. 1,409,260); it reportedly was coined and used with the intent that it have no particular meaning. See Lucia Cucu, The Requirement for Metadata Production Under Williams v. Sprint/United Management Co.: An Unnecessary Burden for Litigants Engaged in Electronic Discovery, 93 Cornell L. Rev. 221 (2007). There still is no single accepted meaningful definition of "metadata," and use of the term as applied to electronically-stored information remains much too imprecise to use as any legal standard. Because this appeal involves a request for a single, specific e-mail, followed by a request for its "metadata," it does not provide a record appropriate for establishing any bright-line rule as to the production of "metadata" under the Public Records Act.

Some electronic "metadata" is analogous to card catalogues and similar systems librarians traditionally have used for cataloging and

retrieving books and other materials.⁴ But there are many other kinds of electronic "metadata" that are not analogous to library catalogues, and which can exist in many forms and many places in an electronic file, computer system, or computer network. As one example, the Sedona Conference® Working Group on Electronic Document Retention and Protection has defined at least seven kinds of electronic "metadata".5 Some types of "metadata" are created by software, without user input, intent, or knowledge, to enhance usability or functionality of the software; some are generated by computer operating systems or networks to track electronically-stored information and the activities of users. "metadata" is stored within electronic files; some is stored externally or even remotely on other computers, computer servers, or computer Some "metadata" is hidden and completely invisible and networks. inaccessible to a computer user without specialized software or expert assistance. Different types of "metadata" are produced by different types

⁴ See Diane Hillman, Dublin Core® Metadata Initiative, Using Dublin Core, § 1.1 (2007) (at http://dublincore.org/documents/usageguide/). This is the type of "metadata" defined in the rules recently adopted by the Washington State Archives to address the retention of electronic records destined for transfer to the state Digital Archives. WAC 434-662-020. See also Washington State Archives, Office of the Secretary of State, "Frequently Asked Questions for Digital WAC 434-662" at 5 (2008) (at http://www.sos.wa.gov/_assets/archives/DigitalArchivesWACfaq.doc). The rules address retention solely for digital archival purposes and do not govern public disclosure or the production of public records under the Public Records Act. The rules were adopted under authority specifically delegated in RCW 40.14, in which the Legislature has delegated to the state and local records committees authority to determine retention requirements for public records. RCW 40.14.060, .070.

⁵ Crowley & Harris, Sedona Conference Glossary at 3, 11, 16, 19, 22, 49, 55.

of software and by different operating systems, and different companies producing a given type of software or system often create different "metadata" to facilitate the operation of their own products.

While some types of "metadata" may provide useful information in some contexts, such as discovery, "metadata" also can be misleading. E-mail systems, for example, "are inherently insecure and unreliable" and the authenticity of e-mail must be established for admission under the rules of evidence. In a collaborative environment, it may not be possible to determine from any available "metadata" who authored a particular document or whether a particular document has been "sabotaged" by an unknown person. Merely opening a file for review (e.g., to determine whether it is responsive to a request or whether any information must be redacted before disclosure) can modify some "metadata", making it useless or misleading for authenticity purposes. 8

⁶ See Kevin F. Brady et al., eds., The Sedona Conference® Commentary on ESI Evidence & Admissibility, 8 Sedona Conf. J. 239, at *4 (Mar. 2008) (at http://www.thesedonaconference.org/dltForm?did=ESI_Commentary_0308.pdf), citing Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 555 (D. Md. 2007). "[S]pecial problems with email may arise when an e-mail recipient attempts to authenticate the message on the basis that it was authored by a particular individual whose name appears in the 'From' field of the header. For example, e-mail may be susceptible to 'spoofing', where the sender of an e-mail uses another's name and makes the message appear to originate from a different location, often through the use of another person's computer." Id. at *6. Such "spoofing" is not particularly difficult to accomplish. Ball, Meeting the Challenge at 13.

⁷ Crowley & Harris, Sedona Conference Glossary at 11.

⁸ Id. at 13.

In short, "metadata" is a popular and convenient term that has no fixed meaning and does not refer to any specific information. A nonspecific request for "metadata" therefore is not a request for an identifiable record under the Act. RCW 42.56.080. Accord Beal v. City of Seattle, 150 Wn. App. 865, 209 P.3d 872 (2009).

2. Most "Metadata" Is Not Related To The Conduct Of Government

Given the existing imprecision and uncertainty as to what "metadata" is, where it can be located, and even whether it exists for specific records, it is not surprising that the Public Records Act does not reference "metadata" or require its disclosure. Since its enactment by initiative in 1972, the Act consistently has focused on access to information "relating to the conduct of government or the performance of any governmental or proprietary function. Compare Laws of 1973, ch. 1, § 2, with RCW 42.17.020(42) and 42.56.010(2). But, with few exceptions, modern "metadata" is not created by government employees using computers, but by the computer programs and systems they are

Most of the increase in the use of electronic records has occurred since the Public Records Act was enacted in 1972. The first capable word processing and spreadsheet applications for desktop computers did not appear until 1979. Graphical interfaces first appeared in the 1980s. Until the early 1990s, e-mail use was confined primarily to the military and academia. See generally Computer History Museum, Timeline of Computer History (at http://www.computerhistory.org/timeline/?category=sl); Ian Peter, The History of E-mail (at http://www.nethistory.info/History%20of%20the%20Internet/email.html); Richard T. Griffiths, History of Electronic Mail (at http://www.let.leidenuniv.nl/history/ivh/chap3.htm).

using. Very little "metadata" is created to accomplish any purpose of government; the vast majority is created and used to accomplish the purposes of the programs and systems that create it. The content, form, extent, and accuracy of that "metadata" may be unknown and unknowable to the user. Such "metadata" is not related to the conduct of government, but to the operation of the computer program or system. Because a reasonable government employee would not know which of this hidden information, if any, is available in the record or how to extract it and provide it to a requester, a request for that information cannot be considered a request for an identifiable public record. *See Bonamy v. City of Seattle*, 92 Wn. App. 403, 410, 960 P.2d 447 (1998), *review denied*, 137 Wn.2d 1012 (1999) (identifiable record is one that is reasonably locatable).

Given the facts of this case, it appears that only the "header metadata" in one e-mail is at issue, and the court of appeals correctly assessed whether it contained information that was related to the conduct of government in determining whether it should be disclosed under the Act. Court of Appeal's decision, 145 Wn. App. at 925, ¶19. However, the court of appeals was uncertain as to whether there were any other kinds of "metadata" that might be associated with the requested e-mail, so it remanded for fact-finding. *Id.* at 924-25, ¶¶18-19. This Court should

decline to allow that remand to become a forensic fishing expedition into unspecified types of "metadata" that may or may not exist (analogous to remanding for forensic analysis of ink or fiber content on a paper document because it may reveal some unspecified information). See Hangartner v. City of Seattle, 151 Wn.2d 439, 448, 90 P.3d 26 (2004) (Public Records Act does not authorize unbridled searches of agency property); Limstrom v. Ladenburg, 136 Wn.2d 595, 604 n.3, 963 P.2d 869 (1998) (Act does not provide right to citizens to "indiscriminately sift through an agency's files in search of records or information which cannot be reasonably identified or described to the agency"). Only in the most abstract or hypertechnical sense can most "metadata" added by computer programs or systems be said to relate to the conduct of government or the performance of a governmental function. In discovery, this "metadata" might be relevant and thus discoverable—but, as shown below, discoverability is not the touchstone for responding to public records requests.

More importantly, this type of "metadata" extraction runs far afield of the fundamental purpose to be served by the Public Records Act. The Act is intended to provide a window on government decision-making, not a fishing expedition to determine what "metadata" Microsoft or Cisco Systems or Juniper Networks has determined should be created or used by

its applications and operating systems. The Legislature has never indicated its intent that the Act require the disclosure of this type of invisible "metadata".

The Court should refrain from issuing any broad mandate as to the treatment of "metadata" or the form of its production under the Public Records Act. While some types of "metadata" may be related to the conduct of government, as the court of appeals found here, other types are not. Any new mandate as to the scope of agencies' public records obligations regarding "metadata" should come from the Legislature after appropriate legislative fact-finding, ¹⁰ not in a case involving a single e-mail and a limited record.

3. The Court Should Refrain From Importing Electronic Discovery Rules Into The Public Disclosure Context

For similar reasons, the Court should not rely on cases involving electronic data discovery to determine standards and obligations regarding public disclosure. As the use of forensic analysis of electronic data has increased in some kinds of civil litigation in federal courts, those courts have begun to address "metadata" in orders responding to discovery disputes. While these cases serve to educate about various types of

¹⁰ See York v. Wahkiakum Sch. Dist. 200, 163 Wn.2d 297, 342, ¶ 88, 178 P.3d 995 (2008) (J.M. Johnson, J., concurring) (noting the important role of legislative fact-finding in policy development).

"metadata" and their use in litigation, these discovery cases cannot be applied directly to the disclosure of public records by public agencies. Discovery and public disclosure are very different in several important ways.

Most notably, the production of records in public disclosure is governed in Washington by the Public Records Act, while discovery is governed by court rules. In federal cases, discovery is limited by the "proportionality" principle, articulated in Fed. R. Civ. P. 26(b)(2)(C). This principle provides that a party need not provide discovery when the potential benefits to the requesting party are outweighed by the burdens or costs involved. There is no "proportionality" principle articulated in the Public Records Act, as this Court long has recognized. See Hearst Corp.

v. Hoppe, 90 Wn.2d 123, 131-32, 580 P.2d 246 (1978) (cost, difficulty,

¹¹ Fed. R. Civ. P. 26(b) was amended in 2006 to address the discovery and use of electronically-stored information.

¹² See, e.g., Kay Beer Distrib., Inc. v. Energy Brands, Inc., No. 07-C-1068, 2009 WL 1649592 (E.D. Wis. June 10, 2009) (refusing to compel production of electronic information collected in preliminary search because costs of further review for privilege, confidentiality, and relevant information were excessive); Dilley v. Metro. Life Ins. Co., 256 F.R.D. 643, 645 (N.D. Cal. 2009) (refusing to require production of "relatively inaccessible" electronic data where "the significance of the discovery to the issues in the present case is substantially outweighed by the burden"); Mancia v. Mayflower Textile Servs. Co., 253 F.R.D. 354, 364 (D. Md. 2008) (ordering parties to "attempt to quantify a workable 'discovery budget' . . . proportional to what [was] at issue in the case"); Oxford House, Inc. v. City of Topeka, 2007 WL 1246200 (D. Kan. 2007) (denying access to deleted e-mail because "the likelihood of retrieving these electronic communications is low and the cost high").

and inconvenience to agency cannot justify failure to disclose public record).

Fed. R. Civ. P. 26(b)(2)(B) provides that a party need not provide discovery of electronically-stored information from sources the party shows are not reasonably accessible because of undue burden or cost, unless the requesting party shows good cause.¹³ In contrast, the Public Records Act does not allow any agency to reject a public records request that is overbroad, RCW 42.56.080, and this Court has rejected any limit on public disclosure based on inaccessibility or undue burden or cost. *Hearst Corp.*, 90 Wn.2d at 131-32. Neither is a person requesting public records required to make any showing of good cause—indeed, the purpose of a request almost always is immaterial to the agency's duty to respond to the request. RCW 42.56.080 (with minor exceptions, requesters "shall not be required to provide information as to the purpose for the request").

Fed. R. Civ. P. 26(b) is silent on the form in which electronically-stored information should be produced. ¹⁴ Fed. R. Civ. P. 34(b) provides that, absent agreement of the parties or a court order, electronic information must be produced in a form in which it is "ordinarily

See, e.g., Zubulake v. UBS Warburg, 217 F.R.D. 309, 318-20 (S.D.N.Y. 2003) (accessibility assessed primarily by expense of production).

See Cucu, 93 Cornell L. Rev. at 224 (rule makers were silent because electronic discovery was such a new and changing area of law that the Civil Rules Advisory Committee was not confident in setting down a firm and inflexible rule).

maintained" or in a "reasonably usable" format, but neither form is intended to mandate production of "metadata". ¹⁵ Rather, the need for "metadata" in this context depends on relevance, which varies substantially depending on the type of electronically-stored information at issue. ¹⁶ But relevance is not an issue under the Public Records Act. *See* RCW 42.56.080 (purpose of request immaterial).

"Mere imperfection" in discovery compliance is not a ground for sanctions. The same is not true under the Public Records Act—penalties and attorney fees are awarded for "mere imperfection" in complying with the act's disclosure requirements. RCW 42.56.550(4); Koenig v. City of Des Moines, 158 Wn.2d 173, 188, 142 P.3d 162 (2006) (requester entitled to monetary penalty whenever agency erroneously denies access to public record); Yousoufian v. Office of Ron Sims, 152 Wn.2d 421, 432-33, 98 P.3d 463 (2004) (same); Amren v. City of Kalama, 131 Wn.2d 25, 37, 929 P.2d 389 (1997) (same).

¹⁵ Thomas Y. Allman, The Impact of the Proposed Federal E-Discovery Rules, 12 Rich. J.L. & Tech. 1, 15 (2006).

See, e.g., Michigan First Credit Union v. Cumis Ins. Soc'y, Inc., 2007 WL 4098213 (E.D. Mich. 2007) (sustaining objection to production "with intact metadata" because "production of this metadata would be overly burdensome with no corresponding evidentiary value"). See also Kentucky Speedway, LLC v. NASCAR, Inc., 2006 WL 5097354 at *8 (E.D. Ky. 2006) ("In most cases and for most documents, metadata does not provide relevant information."); Redgrave, The Sedona Principles at 4 ("In most cases... metadata will have no material evidentiary value").

¹⁷ "[T]he rules of discovery don't require you to do the impossible. All they require is diligence, reasonableness, and good faith." Ball, *Meeting the Challenge* at 6.

Finally, because discovery occurs in active litigation, the court is available to mediate disputes between parties as to all issues related to a discovery request, including relevance, need, burden, availability, cost, and form of disclosure. In sharp contrast, an agency must make its public records determinations without the assistance of a neutral mediator, and judicial review is conducted afterward with penalties and attorney fees available for any disclosure error made by an agency. RCW 42.56.550(4).

The federal discovery rules provide sideboards of relevance and undue burden, with mediation by judges, to control the scope and cost of electronic data discovery. Even with sideboards, electronic discovery in federal litigation has become extraordinarily expensive in some cases because of the need to employ consultants to preserve, extract, and review "metadata" for privilege before producing records in discovery. No such sideboards are present in the Public Records Act; instead, agencies have discretion to determine methods of production that most efficiently and effectively provide requested records. Until the Legislature amends the

^{18 &}quot;[T]he cost of responding to a discovery request can be in the millions of dollars if several years' worth of archived e-mails and files must be located, preserved, restored, sorted through, and collected in a forensically sound manner." Mia Mazza et al., In Pursuit of FRCP 1: Creative Approaches to Cutting and Shifting the Costs of Discovery of Electronically Stored Information, 13 Rich. J.L. & Tech. 11 (2007). "Even a narrowly tailored request for [electronic] information may be so cost-intensive as to surpass the overall value of the litigation in question." Rodney A. Satterwhite & Matthew J. Quantrara, Asymmetrical Warfare: The Cost of Electronic Discovery in Employment Litigation, 14 Rich. J.L. & Tech. 9, 14 (2008).

Act to include scope and cost limits like those provided in the federal discovery rules, the Court should refrain from importing piecemeal into the Public Records Act other substantive standards and duties imposed in the federal electronic disclosure requirements.

IV. CONCLUSION

The Court should not mandate any format for the production of electronic records under the Public Records Act. The Court should hold that a request for an electronic record is not automatically construed under the Act as a request for "metadata" associated with that record, and that a request for nonspecific "metadata" is not a request for an identifiable record as defined in the Act. The proper treatment of "metadata" under the Public Records Act is a question that should be left to the Legislature.

RESPECTFULLY SUBMITTED this 12th day of February, 2010.

ROBERT M. MCKENNA Attorney General

ALAN D. COPSEY, WSBA #23305

Deputy Solicitor General

Attorney for Amicus State of Washington

PO Box 40100

Olympia, WA 98504-0100

(360) 664-9018

alanc@atg.wa.gov